UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/659,985 | 09/10/2003 | Joshua D. Hug | RN131 (2635-004-03) | 4643 |

72455 7590 04/22/2008

RealNetworks, INC.
Graybeal Jackson Haley LLP
155 - 108th Ave NE Suite 350
Bellevue, WA 98004-5973

| EXAMINER | |
|---|---|
| CERVETTI, DAVID GARCIA | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 04/22/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/659,985 | **Applicant(s)**<br>HUG ET AL. | |
| | **Examiner**<br>DAVID CERVETTI | **Art Unit**<br>2136 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on _14 January 2008_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) _15-82_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _15-82_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

## DETAILED ACTION

1. Applicant's arguments filed January 14, 2008, have been fully considered.

2. Claims 15-82 are pending and have been examined. Claims 1-14 have been cancelled.

### *Response to Amendment*

3. The objection to claim 34 is withdrawn.

4. Applicant's arguments with respect to the prior art have been considered but are moot in view of the new ground(s) of rejection.

### *Information Disclosure Statement*

5. It is noted that no Information Disclosure Statement has been filed on this application.

### *Claim Rejections - 35 USC § 102*

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

**7. Claims 39-46, 49-52, 60-70, 79, and 81-82 are rejected under 35 U.S.C. 102(e) as being anticipated by Babowicz et al. (US Patent Application Publication 2005/0229013 A1, hereinafter Babowicz).**

**Regarding claim 39**, Babowicz teaches a system for protecting media content, the system comprising:

a computing device;

media content stored on the computing device;

at least one digital rights management license stored on the computing device and describing allowed uses for the media content;

digital rights management software stored on the computing device and that, when executed by the computing device, causes the computing device to use the digital rights management license to determine whether or not a requested use of the second data is allowed, and to prevent the requested use of the second data if the license does not permit the requested use **(fig. 2, pars. 24-30)**; and

wherein the media content the at least one digital rights management license, and the digital rights management software were installed on the computing device from a single storage medium that contained the content, the license, and the software **(pars. 25-30)**.

**Regarding claim 40**, Babowicz teaches

a first identifier associated with the at least one digital rights management license;

a hard drive, coupled to the computing device;

a second identifier, stored on the hard drive; and

wherein the digital rights management software, when executed by the computing device, causes the computing device to compare the first identifier to the second identifier before allowing a requested use of the media content **(pars. 45-50)**.

**Regarding claim 41**, Babowicz teaches wherein the digital rights management software comprises a generic module and a unique module **(pars. 36-41)**.

**Regarding claim 42**, Babowicz teaches at least one validation code corresponding to at least one predetermined software module; and validation software that, when executed by the computing device, causes the computing device to compute at least one checksum for the at least one software module and compare the at least one checksum against the validation code, to determine if the at least one predetermined software module should be trusted **(pars. 36-41)**.

**Regarding claim 43**, Babowicz teaches the at least one validation code is a cryptographically-signed hash of a canonically-ordered series of bytes from the at least one predetermined software module; and comparing the at least one checksum against the validation code comprises: decrypting the cryptographically-signed hash; performing a hash on the at least one software module; and comparing the results of the two hashes to see if they match **(pars. 36-41)**.

**Regarding claim 44**, Babowicz teaches wherein the storage medium is a compact disc **(abstract)**.

**Regarding claim 45**, Babowicz teaches

a method of transferring digital data from a removable storage medium to a storage device coupled to a computing device, the method comprising:
copying the digital data from the removable storage medium to the storage device;
copying at least one digital rights management license from the removable storage

medium to the storage device, the digital rights management license describing types of access that are allowed for the digital data **(fig. 2, pars. 24-30)**;

copying digital rights management software from the removable storage medium to the storage device, wherein the digital rights management software, when executed by the computing device, causes the computing device to use the at least one digital rights management license to determine whether or not an access to the digital data is permitted **(pars. 25-30)**.

**Regarding claim 46**, Babowicz teaches determining whether or not the computing device has secure playback software that can read the digital data; and installing secure playback software if the computing device does not have the software **(abstract)**.

**Regarding claims 50, 68**, Babowicz teaches

a method of playing media content stored on a removable storage medium the method comprising:

reading digital data stored in a second format and representing all or substantially all of the media content, wherein the removable storage medium also contains digital data stored in a first format that also represents all or substantially all of the media content **(fig. 2, pars. 24-30)**;

determining from at least one digital rights management license whether or not playback of the digital data stored in the second format is allowed **(pars. 27-30)**.

**Regarding claims 52, 70**, Babowicz teaches authenticating digital rights management software that, when executed by a computer, causes the computer to use the at least one digital rights management license to determine whether or not to allow playback of the digital data **(pars. 27-30)**.

**Regarding claim 60**, Babowicz teaches

a method of transferring digital data stored on a removable storage medium to an external device, the method comprising:

loading digital rights management software from the medium;

retrieving a digital rights management license from the medium **(fig. 2, pars. 24-30)**;

using the digital rights management license to determine whether or not a transfer of the digital data to the external device is allowed **(pars. 27-30)**.

**Regarding claim 62**, Babowicz teaches authenticating the digital rights management software **(figs. 2-4, pars. 24-30)**.

**Regarding claim 63**, Babowicz teaches wherein the external device is a compact disc burner **(abstract)**.

**Regarding claim 64**, Babowicz teaches wherein the external device is a portable audio player **(abstract)**.

**Regarding claim 79**, Babowicz teaches transferring at least a portion of the digital data to the external device in response to the determination that the digital rights management license permits the transfer **(pars. 49-53)**.

**Regarding claim 65**, Babowicz teaches translating the at least a portion of the digital data into a format that the external device can read **(pars. 49-53)**.

**Regarding claim 66**, Babowicz teaches transferring the digital rights management software and the digital rights management license from the removable storage medium to the portable audio player **(pars. 49-53)**.

**Regarding claim 67**, Babowicz teaches wherein: the portable audio player contains digital rights management software that is different than the software loaded from the removable storage medium; and

the method further comprises: translating the digital rights management license into a format that the software already on the portable audio player can read; and transferring the translated digital rights management license to the portable audio player **(pars. 43-48)**.

**Regarding claim 81**, Babowicz teaches

a method of playing media content stored on a removable storage medium the method comprising:

reading digital data stored in a first format and representing all or substantially all of the media content, wherein the removable storage medium also contains digital data stored in a second format that also represents all or substantially all of the media content **(fig. 2, pars. 24-30)**;

preventing an audio player configured to read the digital data stored in the second format from reading the digital data in the first format **(pars. 27-30)**.

**Regarding claim 82**, Babowicz teaches wherein the first format comports to the Redbook compact disc standard **(pars. 25-30)**.

**Regarding claims 49, 51, 61, 69**, Babowicz teaches wherein the removable storage medium is a compact disc **(abstract)**.

### ***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**9. Claims 15-38, 47-48, 53-59, 71-78, and 80 are rejected under 35 U.S.C. 103(a) as being unpatentable over Babowicz, and further in view of Hurtado et al. (US Patent 6,611,812, hereinafter Hurtado).**

**Regarding claim 15**, Babowicz teaches

a method of protecting media content stored on a storage medium, the method comprising **(abstract)**:

creating a first session on the medium, the first session containing digital data stored in a first format and representing all or substantially all of the media content, the digital data in the first session being readable by an electronic device configured to read digital data in the first format **(fig. 2, pars. 24-30)**;

creating a second session on the medium, the second session containing digital data stored in a second format and representing all or substantially all of the media content, the digital data in the second session being readable by a media player associated with a computing device and configured to read the digital data in the second format **(fig. 2, pars. 24-30)**;

including on the second session at least one digital rights management license describing allowed uses for the digital-data **(abstract)**;

including on the second session digital rights management software **(pars. 27-30)**; and

preventing the media player associated with the computing device configured to read the digital data in the second format from accessing the digital data in the first format **(pars. 27-30)**.

Babowicz does not expressly disclose encrypting content or encrypting the digital data in the second session so that the digital rights management software does not grant access to the digital data stored in the second session unless the digital rights management software determines that a requested access complies with the allowed uses described in the at least one digital rights management license.

However, Hurtado teaches encrypting content. encrypting the digital data in the second session so that the digital rights management software does not grant access to the digital data stored in the second session unless the digital rights management software determines that a requested access complies with the allowed uses described in the at least one digital rights management license **(fig. 18, col. 83, lines 4-67)**.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add encryption to the system of Babowicz. One of ordinary skill in the art would have been motivated to perform such a modification to further protect the digital data **(Hurtado, col. 5-6, summary)**.

**Regarding claim 27**, Babowicz teaches a compact disc, comprising **(abstract)**:

a first session readable by a compact disc player **(fig. 2)**;

first data representing all or substantially all media content on the compact disc, the first data stored on the first session and protected so that the first data cannot be decoded into a renderable media presentation by an optical media drive **(pars. 27-30)**;

a second session readable by an optical media drive **(pars. 27-30)**;

at least one digital rights management license, written to the second session, and describing allowed uses for the second data **(pars. 27-30)**;

digital rights management software stored on the second session that, when executed by a computer, causes the computer to use the digital rights management license to determine whether or not a requested use of the second data is allowed, and to prevent the requested use of the second data if the license does not permit the requested use **(pars. 27-30)**.

Babowicz does not expressly disclose encrypting content or second data representing all or substantially all of the media content on the compact disc, the second data stored on the second session and encrypted so that the second data cannot be decoded into a renderable media presentation by the compact disc player;

and at least one decryption key stored on the second session and used by the digital rights management software to decrypt the second data.

However, Hurtado teaches second data representing all or substantially all of the media content on the compact disc, the second data stored on the second session and encrypted so that the second data cannot be decoded into a renderable media presentation by the compact disc player;

and at least one decryption key stored on the second session and used by the digital rights management software to decrypt the second data **(fig. 18, col. 83, lines 4-67)**.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add encryption to the system of Babowicz. One of ordinary skill in the art would have been motivated to perform such a modification to further protect the digital data **(Hurtado, col. 5-6, summary)**.

**Regarding claim 16**, the combination of Babowicz and Hurtado teaches wherein encrypting the data comprises: separating the media audio-content into packets of data; encrypting the packets; storing the encrypted packets to the medium; and storing at least one decryption key on the medium such that the digital rights management software, when executed by a computer, causes the computer to use the at least one decryption key to decrypt the packets **(Hurtado, col.17, lines 50-67, col. 18, lines 1-10)**.

**Regarding claim 17**, the combination of Babowicz and Hurtado teaches wherein encrypting the data further comprises: creating at least two encryption keys; for every encryption key, encrypting at least one packet with that key; encrypting every packet with the at least two encryption keys; and wherein the at least one decryption key comprises sufficient decryption keys to decrypt all of the encrypted packets **(Hurtado, col.17, lines 50-67, col. 18, lines 1-10)**.

**Regarding claim 18**, the combination of Babowicz and Hurtado teaches wherein the encryption keys are symmetric, and wherein the method further comprises: generating at least one protection encryption key for each of the at least two encryption keys; encrypting each encryption key with an associated protection encryption key; storing the at least one encrypted encryption key on the medium; and storing at least one protection decryption key on the medium, such that the at least one protection decryption key can be used to decrypt the at least one encryption key **(Hurtado, col.17, lines 50-67, col. 18, lines 1-10)**.

**Regarding claim 19**, the combination of Babowicz and Hurtado teaches wherein: the at least one protection encryption key comprises a generic protection decryption key and a unique protection encryption key; and the at least one protection decryption key comprises a generic protection decryption key and a unique protection decryption key **(Hurtado, col.17, lines 50-67, col. 18, lines 1-10)**.

**Regarding claim 20**, the combination of Babowicz and Hurtado teaches wherein storing the at least one protection decryption key comprises integrating the protection decryption key inside the digital rights management software **(Hurtado, col.85, lines 35-67)**.

**Regarding claim 21**, the combination of Babowicz and Hurtado teaches wherein the digital rights management software is tamper-resistant **(Hurtado, col.87, lines 32-67, col. 88, lines 1-16)**.

**Regarding claim 22**, the combination of Babowicz and Hurtado teaches storing a binding identifier on the medium, wherein the binding identifier is associated with the at least one digital rights management license, and is used by the digital rights management software to determine whether or not to allow the requested access to the digital data in the second session, and wherein the binding identifier cannot be duplicated onto another storage medium **(Hurtado, col.86, lines 1-45)**.

**Regarding claim 23**, the combination of Babowicz and Hurtado teaches storing the binding identifier comprises encrypting together the at least one license and a copy of the binding identifier that is associated with the at least one license; and the digital rights management software compares a decrypted copy of the binding identifier to the binding identifier present on the medium before allowing the requested access **(Hurtado, col.89, lines 1-45)**.

**Regarding claim 24**, the combination of Babowicz and Hurtado teaches wherein storing the binding identifier comprises: creating a license encryption key from the binding identifier; and encrypting the at least one license with the encryption key; and the digital rights management software decrypts the at least one license using a decryption key created from the binding identifier to determine whether or not to allow the requested access to the digital data in the second session **(Hurtado, col.88, lines 33-67)**.

**Regarding claim 25**, the combination of Babowicz and Hurtado teaches wherein: the digital data on the first session comprises a plurality of separate audio recordings; the at least one digital rights management license comprises a plurality of digital rights management licenses; and at least one of the plurality of digital rights management licenses describes allowed uses for a specific recording **(Hurtado, fig. 18, col.83, lines 45-67)**.

**Regarding claim 26**, the combination of Babowicz and Hurtado teaches wherein the medium is a compact disc **(Hurtado, fig. 18)**.

**Regarding claim 28**, the combination of Babowicz and Hurtado teaches wherein the encrypted second data comprises a plurality of encrypted packets of data **(Hurtado, col. 10, lines 1-47)**.

**Regarding claim 29**, the combination of Babowicz and Hurtado teaches wherein the plurality of encrypted packets are encrypted with a plurality of encryption keys, and wherein the at least one decryption key comprises sufficient decryption keys to decrypt all of the encrypted packets **(Hurtado, col.30, lines 34-61)**.

**Regarding claim 30**, the combination of Babowicz and Hurtado teaches wherein the at least one decryption key is integrated inside the digital rights management software **(Hurtado, col.85, lines 35-67)**.

**Regarding claim 31**, the combination of Babowicz and Hurtado teaches wherein the digital rights management software is tamper resistant **(Hurtado, col.87, lines 32-67, col. 88, lines 1-16)**.

**Regarding claim 32**, the combination of Babowicz and Hurtado teaches a binding identifier stored on the compact disc, associated with the at least one digital rights management license, and used by the digital rights management software to determine whether or not to allow the requested use of the second data, wherein the binding identifier cannot be duplicated onto another compact disc **(Hurtado, col.86, lines 1-45)**.

**Regarding claim 33**, the combination of Babowicz and Hurtado teaches the at least one license and a copy of the binding identifier encrypted together and stored on the second session; and wherein the digital rights management software, when executed by the computer, also causes the computer to compare a decrypted copy of the binding identifier to the binding identifier present on the disc before allowing a requested use of the second data **(Hurtado, col.89, lines 1-45)**.

**Regarding claim 34**, the combination of Babowicz and Hurtado teaches wherein: the at least one license is encrypted using an encryption key created by using the binding identifier a seed; and the digital rights management software, when executed by the computer, also causes the computer to decrypt the at least one license using a decryption key created from the binding identifier to determine whether or not to allow a requested use of the second **(Hurtado, col.88, lines 33-67)**.

**Regarding claim 35**, the combination of Babowicz and Hurtado teaches the second data on the second session comprises a plurality of separate audio recordings; the at least one digital rights management license comprises a plurality of digital rights management licenses; and at least one of the plurality of digital rights management licenses describes allowed uses for a specific audio recording **(Hurtado, fig. 18, col.83, lines 45-67)**.

**Regarding claim 36**, the combination of Babowicz and Hurtado teaches wherein the plurality of digital rights management licenses contain a license describing uses for a plurality of the audio recordings in addition to the at least one license that describes uses for a specific audio recording **(Hurtado, fig. 18, col.83, lines 45-67)**.

**Regarding claim 37**, the combination of Babowicz and Hurtado teaches at least one validation code associated with the digital rights management software wherein the at least one code represents a cryptographically-signed hash of a canonical representation of at least one section of the digital rights management software code, and wherein the digital rights management software, when executed by the computer, causes the computer to detect tampering or replacement of the at least one section of code at the time the code is executed by performing a runtime hash of the at least one section of code and comparing the runtime hash to the stored cryptographically-signed hash **(Hurtado, col.87, lines 32-67, col. 88, lines 1-16)**.

**Regarding claim 38**, the combination of Babowicz and Hurtado teaches protected playback software that, when executed by the computer, causes the computer to play the second data **(Hurtado, col.87, lines 32-67, col. 88, lines 1-16)**.

**Regarding claim 47**, Babowicz does not expressly disclose encrypting the at least one digital rights management license, and wherein the copied digital rights management software, when executed by the computing device, causes the computing device to deny access to the digital data on the storage device unless the at least one digital rights license is decrypted.

However, Hurtado teaches encrypting the at least one digital rights management license, and wherein the copied digital rights management software, when executed by the computing device, causes the computing device to deny access to the digital data on the storage device unless the at least one digital rights license is decrypted **(col 47, lines 25-67)**.

The reasoning for combining is the same as that for claim 15.

**Regarding claim 48**, the combination of Babowicz and Hurtado teaches

wherein encrypting the at least one digital rights management license comprises: generating a binding identifier for the storage device; storing the identifier on the storage device; generating an encryption key from the binding identifier; encrypting the at least one digital rights management license using the generated encryption key; and wherein the digital rights management software, when executed by the computing device, causes the computing device to use the binding identifier to create a decryption key for the at least one license **(Hurtado, col. 86, lines 1-45, col. 89, lines 1-45)**.

**Regarding claims 78, 80**, Babowicz does not expressly disclose the digital data stored in the first format is encrypted, and the method further comprises decrypting the encrypted data. However, Hurtado teaches the digital data stored in the first format is encrypted, and the method further comprises decrypting the encrypted data **(Hurtado, col. 86, lines 1-45, col. 89, lines 1-45)**. The reasoning for combining is the same as that for claim 15.

**Regarding claims 53, 71**, the combination of Babowicz and Hurtado teaches wherein the encrypted data comprises a plurality of encrypted packets of data **(Hurtado, col. 10, lines 1-45)**.

**Regarding claims 54, 72**, the combination of Babowicz and Hurtado teaches wherein decrypting the data comprises: locating at least one decryption key on the removable storage medium; and using the at least one decryption key to decrypt the packets of data **(Hurtado, col. 30, lines 34-61)**.

**Regarding claims 55, 73**, the combination of Babowicz and Hurtado teaches the at least one decryption key is itself encrypted with a protection encryption key; and the removable storage medium contains at least one protection decryption key to decrypt the at least one encrypted decryption key **(Hurtado, col. 17, lines 50-67, col. 18, lines 1-10)**.

**Regarding claims 56, 74**, the combination of Babowicz and Hurtado teaches the protection encryption key comprises a generic protection the encryption key and a unique protection encryption key; and the at least one protection decryption key comprises a generic protection decryption encryption key and a unique protection decryption key **(Hurtado, col. 17, lines 50-67, col. 18, lines 1-10)**.

**Regarding claims 57, 75**, the combination of Babowicz and Hurtado teaches wherein the at least one decryption key is symmetric **(Hurtado, col. 17, lines 50-67, col. 18, lines 1-10)**.

**Regarding claims 58, 76**, the combination of Babowicz and Hurtado teaches generating a symmetric playback protection key; encrypting the at least one decryption key with the symmetric key; and wherein decrypting the encrypted packets of digital data stored in the second format further comprises decrypting the at least one encrypted decryption key prior to decrypting the packets of data **(Hurtado, col. 17, lines 50-67, col. 18, lines 1-10)**.

**Regarding claims 59, 77**, the combination of Babowicz and Hurtado teaches playing the encrypted <u>digital data stored in the second format; and </u>deleting the at least one decryption key and the decrypted packets of data from memory **(Hurtado, col. 51, lines 1-67)**.

### *Conclusion*

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID CERVETTI whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.

11. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

12. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/
Examiner, Art Unit 2136